

AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) In a system including a service that is accessed by a user from one or more devices with varying input capabilities, a method for associating multiple credentials with a single user account such that the user may be authenticated with any one of the multiple credentials, the method comprising an authentication system performing acts of:

receiving an authentication request at the authentication system from a desktop computer device, wherein the authentication request includes a first set of credentials of the user, the first set of credentials comprising a username and a password being selected by the user from among a plurality of credentials valid at the authentication system and associated with the user, the credential being chosen by the user based at least partially on the user's device;

validating the first set of credentials provided by the user, wherein the first set of credentials are associated with a single unique user identifier of the user, a single unique user account, and a single unique user profile;

receiving a second authentication request at the authentication system from a cellular phone, wherein the authentication request includes a second set of credentials of the user, the second set of credentials comprising a numeric username and a numeric pin, wherein the numeric username is distinct from the username; and

validating the second set of credentials provided by the user, wherein the second set of credentials are also associated with the single unique user identifier of the user, the single unique user account, and the single unique user profile, such that the user may access the single unique user account by entering either the first set or the second set of credentials.

receiving new credentials from the user, wherein the new credentials are associated with the same unique user identifier of the user, user account, and user profile;

storing the new credentials in a credential store of the authentication system such that the authentication system can authenticate the user to the service when the user provides any one of the multiple credentials associated with the user account; and

providing, in response to the request, the unique user identifier and the user profile to

the device.

2. (Previously Presented) The method as defined in claim 1, wherein the authentication system is a distributed authentication system, wherein the act of receiving an authentication request at the authentication system further comprises an act of determining where to send the credentials for validation.

3. (Currently Amended) The method as defined in claim 2, wherein the act of determining where to send the credentials for validation uses ~~a~~the username of the credentials.

4. (Currently Amended) The method as defined in claim ~~1~~4₆, wherein the act of receiving a new set of credentials from the user further comprises an act of symmetrically associating the new set of credentials with a unique user identifier.

5. (Currently Amended) The method as defined in claim 4, wherein the act of symmetrically associating the new credential with a unique user identifier further comprises an act of associating the new set of credentials with a user account.

6. (Currently Amended) The method as defined in claim 4, wherein the act of symmetrically associating the new set of credentials with a unique user identifier further comprises an act of caching a copy of the unique user identifier with the new set of credentials.

7. (Currently Amended) The method as defined in claim 1, wherein the act of receiving the new set of credentials from the user further comprises an act of asymmetrically associating the new set of credentials with a primary set of credentials, wherein the primary set of credentials is stored in a primary store with the unique user identifier.

8. (Currently Amended) The method as defined in claim 146, further comprising one or more of:

a step for remembering which set of credentials was received in the authentication request;

a step for prompting the user for a more secure set of credentials when the set of credentials received in the authentication request do not meet security requirements of the service, such that the user selects a new set of credentials from among the plurality of sets of credentials valid at the authentication system; and

a step for providing at least one security measure for each set of credentials associated with the user account, wherein the user is not authenticated to a service if the security measure of a particular set of credentials is breached or the user account is locked.

9. (Currently Amended) The method as defined in claim 1, wherein the unique user account corresponds to a service, the method further comprising: In a system that includes multiple services that are accessed by a user over a network such as the Internet, wherein the user accesses the multiple services from one or more devices that have varying input capabilities, a method for accessing a service from a device, the method comprising acts of:

providing multiple credentials to an authentication system, wherein each of the multiple credentials is associated with a user account, a unique user identifier and a user profile that is maintained by the authentication system;

requesting access to a service using a device included in the one or more devices, wherein the service requires that the user be authenticated before access to the service is granted to the user, wherein the device is redirected to the authentication system;

the user selecting an access credential from among the multiple credentials provided by the user to the authentication system, the selection based on at least partially on the user's device to send to the authentication system and entering the access credential selected by the user in the device;

issuing an authentication request to an authentication system, wherein the authentication request includes the access credential selected by the user;

receiving an authentication response from the authentication system, wherein the authentication response includes the unique user identifier that authenticates the user to the service if the access credential selected by the user is validated, the response also including the

user profile; and

sending an authenticated request to the service, wherein the authenticated request includes the unique user identifier and user profile such that access to the service is obtained.

10-21. (Canceled)

22. (Currently Amended) The method as recited in claim 446, wherein the new set of credentials has an associated security level and wherein the user has attempted to authenticate using the first set of credentials and wherein the method further comprises:

associating the new set of credentials with the user account such that the user can be authenticated with both the original credential and the new credentialany of the plurality of sets of credentials,

prior to providing the response, and subsequent to receiving the authorization request, prompting the user for a secure set of credentials that is more secure than the original first set of credentials if the security level of the original first set of credentials is insufficient for a service being accessed by the user, wherein the service is provided with the security level of both the original first set of credentials and the secure set of credentials, but is not aware of either the original first set of credentials or the secure set of credentials.

23. (Currently Amended) The method as defined in claim 22, wherein the step for associating the new set of credentials with the user account further comprises a step for symmetrically associating the original first set of credentials and the new set of credentials with the user account, wherein the user account is cached with each of the original first set of credentials and the new set of credentials.

24. (Currently Amended) The method as defined in claim 23, wherein the step for associating the new set of credentials with the user account further comprises a step for asymmetrically associating the new set of credentials with a primary set of credentials, wherein the primary set of credentials is associated with the user account and wherein the primary set of credentials is cached with each new set of credentials.

25. (Previously Presented) The method as defined in claim 22, further comprising a step for automatically authenticating the user at different services after the user has been authenticated at a first service.

26. (Canceled)

27. (Currently Amended) In a system including a service that is accessed by a user from one or more devices with varying input capabilities, a computer program product for implementing a method for associating multiple credentials with a user account such that the user may be authenticated with anyone of the multiple credentials, the computer program product comprising:

a computer readable storage medium storing computer readable instructions for performing a method comprising:

receiving an authentication request at the authentication system from a desktop computerdevicee, wherein the authentication request includes a first set of credentials of the user, the first set of credentials comprising a username and a passwordbeing selected by the user from among a plurality of credentials valid at the authentication system, the credential being chosen by the user based at least partially on the user's device;

validating the first set of credentials provided by the user, wherein the first set of credentials are associated with a single unique user identifier of the user, a single unique user account, and a single unique user profile, wherein the type of credentials provided by the user are at least partially validated as being of a type associated with the device type such that only credentials of a type associated with the device type are allowed;

receiving a second authentication request at the authentication system from a cellular phone, wherein the authentication request includes a second set of credentials of the user, the second set of credentials comprising a numeric username and a numeric pin, wherein the numeric username is distinct from the username; and

validating the second set of credentials provided by the user, wherein the second set of credentials are also associated with the single unique user identifier of the user, the single unique user account, and the single unique user profile, such that the user may access the single unique user account by entering either the first set or the second set of credentials.

receiving new credentials from the user, wherein the new credentials are associated with the same unique user identifier of the user, user account, and user profile and wherein the new credentials are at least partially validated as being of a type associated with the device type such that only credentials of a type associated with the

device type are allowed;

storing the new credentials in a credential store of the authentication system such that the authentication system can authenticate the user to the service when the user provides any one of the multiple credentials associated with the user account; and

providing, in response to the request, the unique user identifier and the user profile to the device, the unique user identifier wherein the same unique user identifier is provided to the user regardless of the credentials received from the user and the user's device.

28. (Previously Presented) The computer readable storage medium of claim 27, wherein the authentication system is a distributed authentication system, wherein the act of receiving an authentication request at the authentication system further comprises an act of determining where to send the credentials for validation.

29. (Currently Amended) The computer readable storage medium of claim 28, wherein the act of determining where to send the credentials for validation uses thea username of the credentials.

30. (Currently Amended) The computer readable storage medium of claim 2747, wherein the act of receiving a new set of credentials from the user further comprises an act of symmetrically associating the new set of credentials with the unique user identifier.

31. (Currently Amended) The computer readable storage medium of claim 30, wherein the act of symmetrically associating the new credential with the unique user identifier further comprises an act of associating the new set of credentials with a user account.

32. (Currently Amended) The computer readable storage medium of claim 30, wherein the act of symmetrically associating the new set of credentials with the unique user identifier further comprises an act of caching a copy of the unique user identifier with the new set of credentials.

33. (Currently Amended) The computer readable storage medium of claim 27, wherein the act of receiving the new set of credentials from the user further comprises an act of asymmetrically

associating the new set of credentials with a primary set of credentials, wherein the primary set of credentials is stored in a primary store with the unique user identifier.

34. (Currently Amended) The computer readable storage medium of claim 27, wherein the computer readable instructions further comprise instructions for performing the acts of:

remembering which set of credentials was received in the authentication request; and
prompting the user for a more secure set of credentials when the set of credentials received in the authentication request is not sufficient for the service.

35. (Currently Amended) The computer readable storage medium of claim 27, wherein the unique user account corresponds to a service, and wherein the computer readable instructions further comprise instructions for performing the acts of:

receiving an authentication response from the authentication system, wherein the authentication response includes the unique user identifier that authenticates the user to the service, the response also including the user profile; and

sending an authenticated request to the service, wherein the authenticated request includes the unique user identifier and user profile such that access to the service is obtained.
In a system that includes multiple services that are accessed by a user over a network such as the Internet, wherein the user accesses the multiple services from one or more devices that have varying input capabilities, a computer program product for implementing a method for accessing a service from a device, the computer program product comprising:

a computer readable medium having computer executable instructions for performing the method of claim 9.

36-40. (Canceled)

41. (Currently Amended) The method as defined in claim 1, wherein the same unique user identifier is provided to the user regardless of the set of credentials received from the user.

42. (Canceled)

43. (Currently Amended) The method as defined in claim 446, wherein providing the unique user identifier and the user profile to the device comprises sending a cookie containing the unique user identifier and the user profile to the device.

44. (Previously Presented) The method as defined in claim 1, wherein the user profile includes data about the user comprising name, personal information, preferred language, preferences, and location.

45. (Currently Amended) The method as defined in claim 446, wherein the act of validating the first and second sets of credentials provided by the user further comprises an act of the authentication system comparing the first and second sets of credentials selected by the user against the plurality of sets of credentials stored in the credential store to determine validity.

46. (New) The method as defined in claim 1 wherein the user selects which set of credentials to provide from among a plurality of sets of credentials valid at the authentication system and associated with the user, the set of credentials being chosen by the user based at least partially on the user's device, the method further comprising:

receiving a new set of credentials from the user, wherein the new set of credentials is associated with the same unique user identifier of the user, user account, and user profile;

storing the new set of credentials in a credential store of the authentication system such that the authentication system can authenticate the user to the service when the user provides any one of the multiple sets of credentials associated with the user account; and

providing, in response to the request, the unique user identifier and the user profile to the device.

47. (New) The computer readable storage medium of claim 27, wherein the user selects which set of credentials to provide from among a plurality of sets of credentials valid at the authentication system and associated with the user, the set of credentials being chosen by the user based at least partially on the user's device, wherein the computer readable instructions further comprise instructions for performing the acts of:

receiving a new set of credentials from the user, wherein the new set of credentials is

associated with the same unique user identifier of the user, user account, and user profile;
storing the new set of credentials in a credential store of the authentication system such that
the authentication system can authenticate the user to the service when the user provides any one of
the multiple sets of credentials associated with the user account; and
providing, in response to the request, the unique user identifier and the user profile to the
device.

48. (New) In a system including a service that is accessed by a user from one or more devices with varying input capabilities, a method for associating multiple credentials with a single user account such that the user may be authenticated with any one of the multiple credentials, the method comprising an authentication system performing acts of:

receiving an authentication request at the authentication system from a first computer, wherein the authentication request includes a first set of credentials of the user;

validating the first set of credentials provided by the user, wherein the first set of credentials are associated with a single unique user identifier of the user, a single unique user account, and a single unique user profile;

receiving a second authentication request at the authentication system from a second computer, wherein the authentication request includes a second set of credentials of the user, the second set of credentials being different than the first set of credentials; and

validating the second set of credentials provided by the user, wherein the second set of credentials are also associated with the single unique user identifier of the user, the single unique user account, and the single unique user profile, such that the user may access the single unique user account by entering either the first set or the second set of credentials.

49. (New) The method of claim 48, wherein the first and second computer are the same computer, and wherein the first set and second set of credentials comprise a username and password, and wherein the username of the first set of credentials is different than the username of the second set of credentials.

50. (New) The method of claim 49, wherein the username of first set of credentials is an email address having a first domain and the username of the second set of credentials is an email address having a second domain that is different than the first domain.